Security incidents management in a grid environment

Romain Wartel, CERN IT

On behalf of the EGEE Operational Security Coordination Team

Presented by Markus Schulz, CERN IT

CHEP 2007, Victoria, BC

3rd September 2007

www.eu-egee.org

Computer security incident

- **What is a "Security Incident"?**

  A security incident is the act of violating an explicit or implied security policy

- **What can motivate attackers?**
  - **Money (and little risk of being caught)**
  - **Less likely: political motivation, challenge, ego, fame, etc.**

- **How do attackers often proceed?**
  - **Most attacks are partly/fully automated**
  - **First find an entry point (weak network service, stolen credentials, etc.)**
  - **Install necessary toolkit to maintain a 'quiet' access**
  - **Implant payload (DDOS, Botnet, SPAM engine, etc.)**
  - **Harvest additional credentials**

Exposure

- Grids are valuable to attackers:
  - Large numbers of distributed hosts
  - High availability
  - High throughput network
- Grids are also particularly exposed
  - Transparent access/attack propagation from one site to the other
  - Large number of identical hosts
  - Heterogeneous skills, staffing and security standards
- A few incidents happen per year within Grids
- So far no “grid incident” … but will happen
(= where the grid is the attack vector)

Incident response policy

- Response to security incidents is primarily guided by policies

- Grid participants are bound to (at least) two different incident response policies:
  - Local incident response policy
  - "LCG/EGEE Incident Handling and Response Guide" (JSPG) Based on the Open Science Grid, Approved by WLCG Management Board on 28 Nov 2005:

    http://cern.ch/proj-lcg-security/docs/LCG_Incident_Response.asp

Incident response procedure for grid hosts

This procedure is provided for guidance only and is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between the sites. It is based on the EGEE Incident Response policy (available at https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf) and is intended for Grid site security contacts and site administrators.

A security incident is the act of violating an explicit or implied security policy (ex: your local security policy, EGEE Acceptable Use Policy - https://edms.cern.ch/document/428036/3). When a security incident is suspected, the following procedure should be used:

1- Contact immediately your local security team and your ROC Security Contact.

2- In case no support is shortly available, whenever feasible and if you are sufficiently familiar with the host/service to take responsibility for this action, try to contain the incident, for instance by unplugging the network cable connected to the host. Do NOT reboot or power off the host.

3- Assist your local security team and your ROC Security Contact to confirm and then announce the incident to all the sites via project-egee-security-csirts@cern.ch.

Incident response procedure for grid hosts

4- If appropriate:

*** report a downtime for the affected hosts on the GOCDB**

*** send an EGEE broadcast announcing the downtime for the affected hosts**

Use "Security operations in progress" as the reason with no additional detail both for the broadcast and the GOCDB.

5- Perform appropriate forensics and take necessary corrective actions

*** If needed, seek for help from your local security team or from your ROC Security Contact or from project-egee-security-support@cern.ch**

*** If relevant, send additional reports containing suspicious**

patterns, files or evidence that may be of use to other Grid participants to project-egee-security-contacts@cern.ch. NEVER send potentially sensitive information (hosts, IP addresses, usernames)

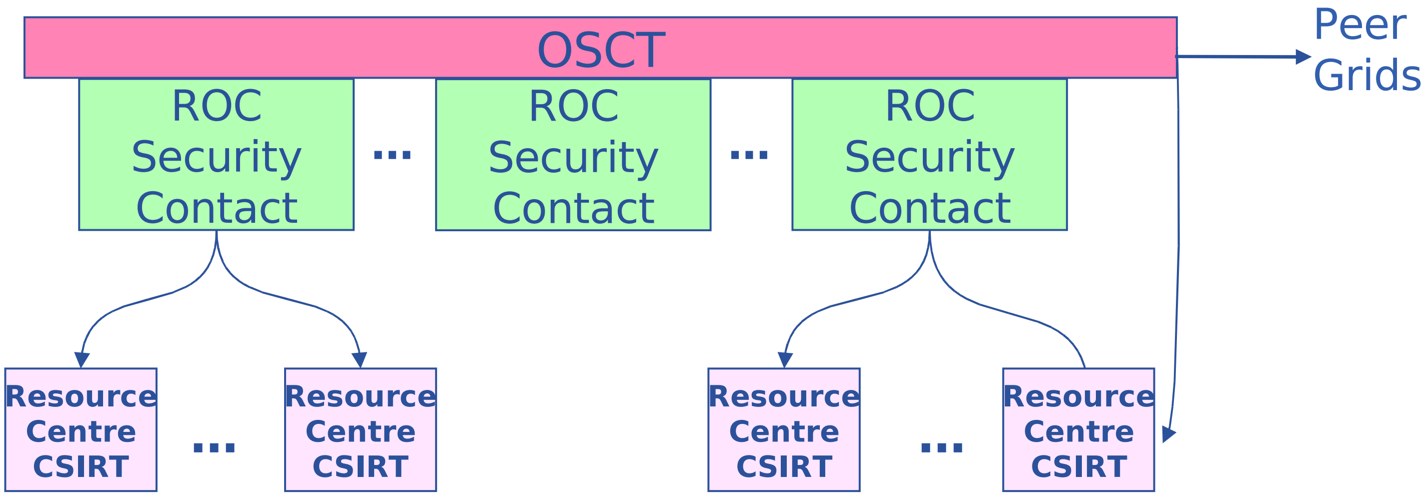
without clearance from your local security team and/or your ROC Security Contact.

6- Coordinate with your local security team and your ROC Security Contact to send an incident closure report within 1 month following the incident, to all the sites via project-egee-security-contacts@cern.ch, including lessons learnt and resolution.

7- Restore the service, and if needed, send an EGEE broadcast, update the GOCDB, service documentation and procedures to prevent recurrence as necessary.

Incident response coordination

- ROC Security Contacts are part of the EGEE Operational Security Coordination Team (OSCT)
- Small incidents coordination: first site reporting the attack
- Large incidents coordination: ROC Security Contact on duty



Incident response coordination

A large part of IR coordination consists in managing the flow of information

- **The role of the coordinator is to:**
  - **Process the available information as soon as possible and follow the most likely leads**
  - **Provide accurate information to the sites**
  - **Contact and follow up with the relevant CERTs/CSIRTs**
  - **Ensure the process does not stall**

- **The objective is to:**
  - **Understand what was the vector of attack (ex: entry point)**
  - **Ensure the incident is contained**
  - **Establish a detailed list of what has been lost (ex: credentials, data)**
  - **Take corrective action to prevent re-occurrence**

Trust and leaks

- **Main issues:**
  - **It is essential to establish and maintain trust between the sites**
  - **Obtain relevant and accurate information and collaboration from all possibly affected sites**
  - **Cope with the information flow (large incidents) (during a recent multi-site incident, the coordinator had to process 500+ incoming emails during the first 5 days, including 280 at day 3)**
  - **Redistribute the information with an appropriate level of details**
  - **Prevent information leaks, which are a serious problem. They can discourage other sites from sharing their findings in the future and expose sensitive information (personal details, etc.)**

Other issues

- **Small sites vs big sites**
  - **Incidents at big sites more spectacular and likely to attract attention**
    Deaths caused by sand holes (16) vs Shark Attacks (12) in the US (1990 – 2006)
  - **But small inexperienced sites are an easier target for attackers…and there are many!**
  - **Small inexperienced sites more difficult to reach (training, best practice, monitoring)**

- **It is difficult to build security expertise in the community**

Security incident prevention

The EGEE Operational Security Coordination Team has three main activities:

- **Incident Response improvement**
  - **Security service challenges (SSC)**
  SSC1, SSC2, *SSC3 (in work)*
  - **IR channels (lists, IM)**
  - **IR Scenarios**

- **Incident detection and containment (=monitoring)**
  - **Several monitoring tools available to the sites**
  - **SAM Security Tests (pilot stage)**

- **Incident prevention**
  - **Best practice**
  ex: https://cic.gridops.org/index.php?section=roc&page=securityissues
  - **Training (2 sessions for site admins at EGEE 07!)**

Conclusion

- Incident response policies and procedures are well established
- Tests are performed on a regular basis
- But building trust between the sites and increasing security awareness at the weakest sites remains difficult
- We expect more sophisticated attacks, but experience shows that basic advice still need to be repeated
- Still a lot to do for prevention and detection
- Security in the Grid heavily relies on the involvement of the sites